Protecting Internet Users, Prosecuting Cyber Crime and Other Web Exploitation

Along with millions of New Jerseyans who use the Internet each day for legitimate purposes, there are others who exploit it for illegal or unethical activities, including: distribution of child pornography, identity theft, the sabotaging of on-line businesses via "hacking," and the turning of a profit through misleading representations and hard-to-identify user redirection programs.

In 2005, the Attorney General's Office continued its vigilance against cyber crime and fraud, using an array of strategies to identify and prosecute Internet users who broke the law and, elsewhere, putting a halt to practices that were exploitative and unethical — if not outright fraudulent.

Operation Guardian: Attacking the Menace of Child Pornography

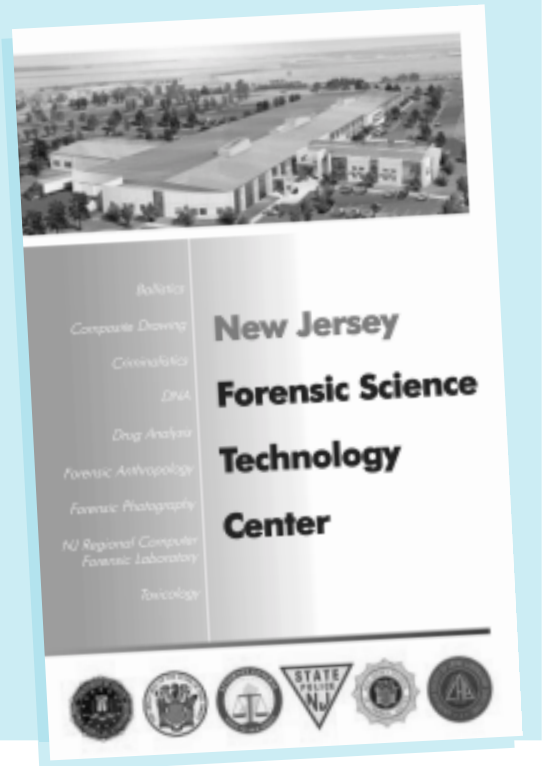
One of the landmark achievements announced in 2005 by Attorney General Harvey was Operation Guardian, an extensive cyber child-pornography investigation spearheaded by the Divisions of State Police and Criminal Justice. As a result of Operation Guardian, 39 people were arrested on charges relating to the possession and distribution of child pornography. Those charged in connection with Operation Guardian ranged in age from 14 to 61, and included a high school hockey coach, an attorney and a pediatric neurosurgeon.

In addition to the arrests, detectives seized computers containing many disturbing "still" photos and video images of child pornography, including video clips of a Georgia man molesting and raping a 5-year-old girl. (Via the Internet and other means, James Bidwell, of Toccoa, Ga. had circulated in United States, Canada and England a video of himself raping the child. Although his video continued to circulate, Bidwell began serving a 45-year prison term in 2002 after pleading guilty to child molestation and rape charges lodged in Georgia, as well as to certain federal crimes.)

The National Center for Missing and Exploited Children lauded the effort as "a tremendous example of how improved technology, law enforcement training, and teamwork can make a difference."

According to Attorney General Harvey, the key to Operation Guardian was the use of comparatively new technology that enabled law enforcement to detect child pornography files shared over the Internet, and trace them to computers on which they were stored. In a solid example of multi-jurisdictional cooperation, the investigation had its roots in Iowa, where a Special Agent with the Iowa Internet Crimes Against Children Task Force had made innovative use of the "file sifting" technology. During a two-day period, the software detected images of child pornography and traced them to 42 computer addresses in New Jersey. Evidence indicated that those New Jersey computer addresses had either received the child pornography files or offered to circulate them, or both. New Jersey State Police then worked with Deputy Attorneys General assigned to the Division of Criminal Justice within the Attorney General's Office to prepare subpoenas that led to search warrants.

In addition to the seizure of computers and child pornography files, Operation Guardian also resulted in the seizure of weapons — including some assault rifles — and some illegal drugs. Spin-off investi-



gations prompted by Operation Guardian continue in New Jersey as of this writing.

Agencies that worked with the New Jersey Attorney General's Office and State Police on Operation Guardian included the FBI, County Prosecutor's Offices throughout the state, approximately 35 municipal police departments in New Jersey, the U.S. Department of Homeland Security's Child Exploitation Group, the National Center for Missing and Exploited Children, and the New Jersey Regional Computer Forensic Laboratory (RCFL).

Located in Hamilton Township, Mercer County, the RCFL is a joint endeavor that combines the resources of the Attorney General's Office, the FBI and local law enforcement agencies. At the RCFL, highly-trained law enforcement personnel work as computer forensic examiners in support of investigations into a host of unlawful activities including: terrorism, financial fraud, identity theft, illegal "hacking" into private or restricted data bases, distribution of child pornography, and on-line luring by sexual predators.

Identifying, Ending Exploitative Internet Business Practices

Under an agreement announced by Attorney General Harvey in 2005, Alyon Technologies, Inc., a North-Jersey-based Internet company, was required to change its practices to ensure that unwitting consumers were not linked in the future to pornographic "pop-up" images, and were not billed for Web-based services they never requested.

In May 2003, the State filed a three-count complaint against Alyon alleging that the company had engaged in fraudulent billing practices by switching Internet users to its network so as to bill them for its services — even though the users did not request those services.

Prior to an investigation by the Attorney General's Office, the State had received more than 700 complaints about Alyon — more than half of them from New Jersey residents — while states throughout the nation had also reported receiving high numbers of complaints.

Typically, complainants reported receiving bills from Alyon or its billing agent — often in the $150 range — for access to on-line pornography. In most cases, the consumers denied accessing pornography, and said they had never authorized Alyon to charge them for on-line services.

Prior to the actual filing of a State complaint, some Web users had complained that they — and sometimes their children — had encountered pornographic "pop-up" images from the Alyon network while using Web sites that featured music or games.

The billing by Alyon of Internet users for services not requested, as well as incidents in which unsolicited materials "popped up" on computer screens, appears to have been caused by flaws that existed in a proprietary computer program used by Alyon. Specifically, the system could not detect or deter Internet use by minors or other unauthorized users, and sometimes generated incorrect billing due to database inaccuracies.

Under the agreement negotiated by the Attorney General's Office (22 other states signed onto the agreement), Alyon was prohibited from billing minors for its Internet services. The agreement also required that the company provide full cash refunds to all consumers who had submitted a complaint about Alyon services billed before June 15, 2003, and who had already paid. Regarding consumers who were billed prior to June 15, 2003 and refused to pay, Alyon was required to cancel their debt and halt all related collection activities.

Other cyber-crime cases from 2005 included:

❖ Youth Gets Prison for "Hacking": In August 2005, a 17-year-old Middlesex County youth was sentenced to five years in State Prison after being waived up to adult court and pleading guilty to sabotaging an on-line sports clothing business through "hacking." Jasmine Singh, of Edison, was also ordered by Superior Court Judge Frederick DeVesa to pay $35,000 in restitution. Singh admitted in court to using a "bot net" to play havoc with the Internet server used by an on-line "retro" sports jersey seller in Burlington County. The constant Web site problems caused by Singh's hacking essentially halted the on-line seller's operation. Investigation revealed that Singh, who was hired by a competing retro-sports-jersey merchant, used his hacking prowess to direct computers around the globe to flood the Burlington County operator's computer with data.

❖ Man Pleads Guilty to Theft Via On-Line Auctions: In January 2005, the Division of Criminal Justice obtained a guilty plea to charges of theft by deception from 26-year-old Wayne J. DeVita of Lincroft, Monmouth County. DeVita had been charged with stealing more than $50,000 from unwitting persons around the country who believed they were legitimately buying from him electronic merchandise — computers, scanners, printers, etc. — via the Internet auction sites e-Bay and Yahoo. DeVita admitted in court that he did not possess, and could not obtain, the merchandise he'd advertised, but had nonetheless collected advance cash payments from unsuspecting buyers on 22 different occasions. No merchandise was ever delivered, and cash payments were not returned.

Kid porn arrest stuns community

84-year-old man charged after Operation Guardian raid

By JOE ZEDALIS
STAFF WRITER

LONG BEACH TOWNSHIP — Residents expressed surprise and dis-

Arnold Boulevard in the High Bar Harbor section, was arrested Tuesday by state and local police. Authorities said he had nu-

who identified herself as Beaumont's wife, Peggy, speaking through a front window at Beaumont's home, said they did not want to talk about the

adults and juveniles, including several from Monmouth and Ocean counties, police said.

"I would never have guessed something like this in a million years,"

in child porn probe

APE VICTIM WAS 5: Video was sent on Net

RAPIST IN PRISON: He got 45 years in Ga.

By MARGARET F. BONAFIDE
STAFF WRITER

orities arrested 39 people from the state — including five from uth and Ocean counties — follow- nvestigation into the sharing, via rnet, of a video clip showing the a 5-year-old girl.

clip was originally made by a a man who is now in prison, au- s said. The success of the investi-

raphy investigations in state history — was attributed to file-sifting technology used by a Wyoming task force that deals with crimes against children.

"The content is sick. Our detectives have seen it," said Col. Joseph "Rick" Fuentes, superintendent of the New Jersey State Police.

The arrests were made in 19 of the state's 21 counties. Suspects include a pediatric neurologist, a high school hockey

See Child porn, Page A7

Of the 39 people arrested during "Operation Guardian," five were from Monmouth and Ocean counties:

- RIGOBERTO GARRO, 40, EATONTOWN
- ADRIAN MENDOZA, 21, NEPTUNE
- FREDERICK KRAGE V, 21, JACKSON
- MATTHEW FOBERG, 20, LAKEWOOD
- UNNAMED JUVENILE, 14, BRICK

Newark housing official indicted over child porn

Former counsel allegedly downloaded images at work

BY JEFFERY C. MAYS AND KATIE WANG
STAR-LEDGER STAFF

The former general counsel for the New- rk Housing Authority has been indicted for llegedly downloading and watching more han 70 images of child pornography on his overnment-owned computer while at work, ute officials said yesterday.

Frank L. Armour, 64, of East Hanover was licted for possession of child pornography

ing authority by the U.S. Department of Housing and Urban Development and is in danger of being taken over by the federal government.

Armour worked at the agency for more than 18 years before retiring March 1, 2004. The indictment alleges he downloaded and viewed the pornographic images depicting nude boys and girls and adults